Approved for public release; distribution is unlimited.

Data Fusion in Offensive and Defensive Information Operations

Ed Waltz
Veridian Systems
Information Technology and Applied Sciences Sector
P.O. Box 134008
Ann Arbor, MI 48113-40008
waltz@erim-int.com   734-994-1200 ext. 2618

Abstract

The conduct of offensive and defensive Information Operations (IO) require coordinated targeting and protection, respectively, across physical, information and even cognitive domains. Even the specific IO activities of Computer Network Defense (CND) and Computer Network Attack (CNA) require the close coordination of activities across all three domains to encompass physical processing assets, information creation, flows and stores, and the cognitive behaviors of human network administrators and operators. This paper describes the role of data fusion to provide intelligence for IO and to conduct both offensive operations (OIO) and defensive operations (DIO). We build on prior papers that have introduced the concept of a three-domain model of IO targets, and the general application of data fusion to the more abstract functions of IO. These functions require the fusion of both quantitative and qualitative data (e.g. numerical and text data, respectively) to develop models of physical, symbolic and cognitive IO targets and situations. This paper describes conceptual implementations of data fusion structures to model and understand OIO and DIO targets within the domains of reality.

Information Operations within JV 2020

Information Operations (IO) are those actions taken to affect an adversary's information and information systems, while defending one's own information and information systems.[1] The recently released Joint Vision 2020 describes the Joint Chiefs of Staff view of the ultimate purpose of IO as "to facilitate and protect U.S. decision-making processes, and in a conflict, degrade those of an adversary." [2] The Vision builds on the earlier JV2010[3] and retains the fundamental operational concepts, two with significant refinements that emphasize IO. The first is the expansion of the Vision to encompass the full range of operations (non-tradition, asymmetric, unconventional ops), while retaining warfighting as the primary focus. The second refinement moves Information Superiority concepts beyond technology solutions that deliver information to the concept of superiority in decision-making. This means that IO will deliver increased information at all levels and increased choices for commanders. Conversely, it will also reduce information to adversary commanders and diminish their decision options

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)
01-01-2001

2. REPORT TYPE
Conference Proceedings

3. DATES COVERED (FROM - TO)
xx-xx-2000 to xx-xx-2000

4. TITLE AND SUBTITLE
Data Fusion in Offensive and Defensive Information Operations
Unclassified

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Waltz, Ed ;

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Veridian Systems
Information Technology and Applied Sciences Sector
P.O. Box 134008
Ann Arbor, MI48113-4008

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
Director, CECOM RDEC
Night Vision and Electronic Sensors Directorate Security Team
10221 Burbeck Road
Ft. Belvoir, VA22060-5806

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES
See Also ADM201258, 2000 MSS Proceedings on CD-ROM, January 2001.

14. ABSTRACT
The conduct of offensive and defensive Information Operations (IO) require coordinated targeting and protection, respectively, across physical, information and even cognitive domains. Even the specific IO activities of Computer Network Defense (CND) and Computer Network Attack (CNA) require the close coordination of activities across all three domains to encompass physical processing assets, information creation, flows and stores, and the cognitive behaviors of human network administrators and operators. This paper describes the role of data fusion to provide intelligence for IO and to conduct both offensive operations (OIO) and defensive operations (DIO). We build on prior papers that have introduced the concept of a three-domain model of IO targets, and the general application of data fusion to the more abstract functions of IO. These functions require the fusion of both quantitative and qualitative data (e.g. numerical and text data, respectively) to develop models of physical, symbolic and cognitive IO targets and situations. This paper describes conceptual implementations of data fusion structures to model and understand OIO and DIO targets within the domains of reality.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

a. REPORT	b. ABSTRACT	c. THIS PAGE
Unclassified	Unclassified	Unclassified

17. LIMITATION OF ABSTRACT
Public Release

18. NUMBER OF PAGES
14

19. NAME OF RESPONSIBLE PERSON
Fenster, Lynn
lfenster@dtic.mil

19b. TELEPHONE NUMBER
International Area Code
Area Code Telephone Number
703767-9007
DSN
427-9007

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39.18

In three prior papers, we have introduced the role of data fusion as critical support to decision-making in information operations, asserting:

- Data fusion is the critical nodal process of command and control (C2) systems, making it both a weapon and target of IO[4],
- IO brings new technology challenges to data fusion and data mining, highlighting the needs to: 1) apply fusion across three domains of human reality, 2) fuse both quantitative and qualitative data sources rather than just quantitative sources , and 3) integrate data fusion and mining into the intelligence enterprise environment as common, interoperable processes [5],
- Information security in these operations is essential at the policy level, as well as the operational level and in the technology base [6].

Core to these concepts and challenges was the notion that IO uniquely requires the coordination of intelligence, targeting and security in three fundamental realms, or domains of human activities[7]:

- The ***Physical*** domain includes physical objects: military facilities, lines of communication, vehicles, aircraft, missiles, and personnel make up the principal target objects of military data fusion. The "orders of battle" that measured Cold War military strength were determined by counting missiles, warheads, tanks and trucks -- all objects of the physical world.
- A more abstract domain, though, is the ***Symbolic*** domain -- the realm of information. Words, numbers, graphics, all encode and represent the physical world, storing and transmitting it in electronic formats, radio and TV signals, the Internet, newsprint and other forms. This is the domain that is expanding at unprecedented rates, as global ideas, communications and descriptions of the world are being represented in this domain. The domain, also described as the "infosphere" or "cyberspace" has become the principal means by which humans shape their perception of the world.
- The ***Cognitive*** domain is the realm of human thought. This is the ultimate locus of all information flows. The individual and collective thoughts of government leaders, and populations at large form this realm. Perceptions and decisions -- and the effects on our nation are formed in this cognitive realm. This is the ultimate target of our adversaries: the realm where uncertainties, fears, panic and terror can coerce and influence our behavior.

These three domains are not arbitrary; even early philosophers have recognized them as the basic components of our knowledge. Aristotle, an empiricist, identified these three domains in his Metaphysics, written in 350 B.C. He distinguished physical objects, and the abstractions (ideas) that the mind creates once the senses perceive the object. He further distinguished the words that the mind creates to symbolize or represent the abstractions of the mind. He further distinguished three processes of the intellect that manipulate these domains:

- *Apprehension* is the process by which the mind perceives and understands the sensed physical object, and creates a mental abstraction. (Physical-to-cognitive object mappings are formed.)
- *Predication* is the process of making declarations or propositions about the object – characterizing the object and its behavior. (Cognitive-to-symbolic mappings are created.)
- *Reasoning* is the process, then, of applying logical principles to the propositions to create new conclusions, or syllogisms. Here, Aristotle recognized the methods of deduction and induction. (Symbolic logic draws new conclusions about cognitive and physical objects.)

More recently, mathematician and logician C.S. Peirce (1839-1914) developed a mathematical theory of signs, or semiotics[8]. More explicitly than Aristotle, Peirce's logic distinguished a "triad" of relationships between the physical object, the symbolic sign that represents it and the cognitive thought in the mind:

> Indeed, representation necessary involves a genuine triad. For it involves a sign, or representamen, of some kind, inward or outward, mediating between an object and an interpreting thought.[9]

The primary emphasis of data fusion work to date has focused on the physical domain – physical military targets (aircraft, ships, ground vehicles and personnel), and physical situations (the positions and courses of action of the physical targets.) This paper emphasizes the need to recognize that there also exist targets, target states, observable phenomena and feasible detection and tracking methods in the symbolic and cognitive realms as well (Figure 1). It is these kinds of targets that are the focus of interest in the IO disciplines of Computer Network Attack/Defense (CNA/CND) and the perception management disciplines of PsyOps/Deception, respectively.

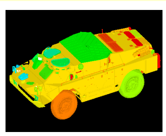
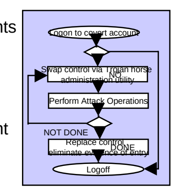
DOMAIN:	PHYSICAL	SYMBOLIC	COGNITIVE
Target Objects	•Vehicles •Facilities	•Packets •Sessions	•Mental States •Ideas
Phenomena Domain	•Laws of Physics	•Network routing, stack and op system protocols	•Human Cognition
Sensors	•EO,IR,SAR, spectral sensors	•SIGINT, NETINT, intrusion sensors	•No direct sensors
States, Feature Complexities	•Physical components •Sensor perspective of target •Target articulations •Environmental signature variance 	•Data components •ISO layer of target and form •Target transformation •Net environment •Signature variance 	•Mental components •Mental states •Cultural, cognitive biases •Behavioral phenomena 
Detection Methodology	•Signature pattern matching •Model-based matching	•Data pattern matching •Model-based matching	•Behavior pattern matching •Cognitive model matching
	Fusion of Data Across three-Domains to Model the "3D Target"		

Figure 1- Representative Targets, States and Observable Phenomena in Three Domains

Current IO concepts have appropriately emphasized the targeting of the second domain – especially electronic information systems and their information content. The expansion of networked information systems and the reliance on those systems has focused attention on network centric forms of warfare. Ultimately, though, IO must move toward a focus on the full integration of the cognitive realm with the physical and symbolic realms to target the human mind[10]. Recent studies within the DoD are moving toward this focus.[11] U.S. Joint Doctrine for Information Operations cites Sir Basil Hart's 1944 insightful assertion that: "The real target in war is the mind of the enemy commander, not the bodies of his troops." [12] Yesterday's emphasis on physical military operations are giving way to today's emphasis on operations in the information realm. Future operations will target all three realms in an integrated fashion. Psychological Operations (PSYOPS) and military deception operations have always targeted the minds of foreign populations and military units, respectively, but the disciplines have not yet achieved full integration with military operations, let alone preeminence. These disciplines, once fully integrated will allow precision cognitive operations.

IO operational concepts that target the human mind and its supporting information systems uniquely refocus the need for data fusion to model the other two domains beyond the physical: electronic information systems and decision-makers' minds[13]. This paper describes the means by which data fusion can play a crucial role in understanding and modeling of the complete system or complex of the targets of IO: the interrelated systems of physical behavior, information perceived and exchanged, and the perception and mental states of decision-makers.

The Impact of IO on Decision-Making

The focus of Defensive IO (DIO) is to enable U.S. leadership to make timely, fully informed and effective decisions that will lead to their objective. The focus of Offensive IO (OIO) is to prevent foreign leaders from doing the same, and in fact to influence to their decisions to favor U.S. goals. The means of doing this encompasses a wider spectrum of methods and operations than traditional military operations, all integrated by IO. This change in warfare has not been unnoticed by foreign observers. In the widely read study, *Unrestricted Warfare*, Chinese military analysts, Liang and Xiangsui have noted,

> "… the new principles of war are no longer 'using armed forces to compel the enemy to submit to one's will,' but rather are, 'using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests." This represents change. A change in war and a change in the mode of war occasioned by this."[14]

Compelling the adversary to accept one's interests has traditionally included alternatives ranging from inducement (diplomacy) to violent coercion (war)[15]. The emergence of a global information infrastructure, the increasing dependence on that infrastructure for commerce and national governance and the increasing empowerment of individuals with access to information have expanded these alternatives to allow IO to become a powerful tool of inducement and coercion.

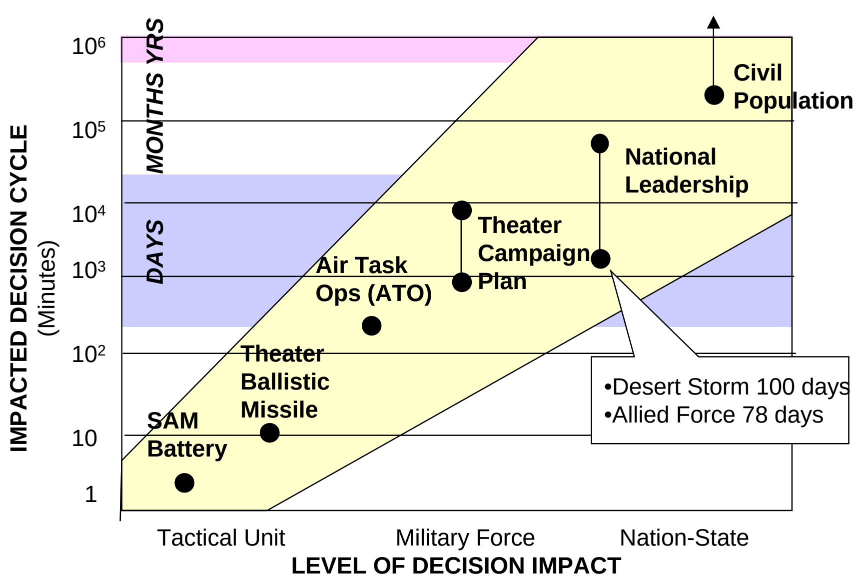


Figure 2 – The Range of Decision Process Targets of IO

The challenge of coercion can be illustrated by considering the increasing difficulty of impacting adversary operations, ranging from tactical military units to national policy, and the affected decision cycles (Figure 2). Tactical attacks (both physical and electronic) on surface to air (SAM) batteries, for example can provide immediate results, influencing air defense command decision-making which has a cycle time on the order of seconds to a few minutes. Theater-level campaign planing decisions require days, like the 24 hour Air Tasking Order (ATO) cyclic and impacts on that planning and decision-making have wider ranging, though more delayed effects. Influencing major national decisions or even large civil populations may require months, or even years to influence large population consensus and group decisions. (Operations Desert Storm and Allied Force required 100 and 78 days, respectively, to coerce national leadership decisions to reverse absolute national policy. In neither case has the civil population, to date, successfully decided and overthrown the dictatorial leaderships. This points out that influencing decision-making is a necessary condition, but must be matched with capability.)

At the most complex decision-making influence toward nation-state leadership, coercion escalates from diplomacy to war (Table 1), and the range of coercive IO options likewise increase. The middle option, coercive inducement is characterized by stabilizing crises as conflict emerges from the mutually exclusive positions of competing parties [16]. The diplomacy and coercive inducement phases are characterized by coercion by "confrontation" while the violence phase is characterized by the application of degrees of "shock and awe" to bring the target to a desired decision[17].

Table 1 – The Escalation of Coercion and the Role of IO

	Diplomacy	**Coercive Inducement**	**Violent Coercion**
Means of Coercion	Political, economic and hortatory persuasion	Stabilize, contain crisis (without forming any position)	• Intimidation (threat of force) then, • Limited coercive action then, • War to submission
The Coercive Role of IO	• Psychological Operations • Economic Network Operations	• Psychological Operations • Economic Network Operations • Military Deception • Military Computer Network Attack	• Psychological Operations • Economic Network Operations • Civil Network Operations • Military Deception • Military Electronic Warfare • Military Computer Network Attack
Psychological Objective	Confrontation		Shock and Awe

In each of the escalating coercive roles of IO, the IO operator must understand the targeted human decision-makers (individuals or organizations). But the operator must also understand the relationships between actions taken against physical objects (e.g. military or civil infrastructure targets) or information system targets (e.g. computer networks) to influence the targeted human minds. This understanding requires means of surveillance and modeling of the physical and symbolic targets and their interaction, as well as the targeted decision-makers.

Data Fusion in Defensive and Offensive IO

Information operations require the surveillance of symbolic and cognitive threats (targets) in addition to the traditional surveillance of physical threats to information and information systems. These surveillance functions generally provide:

- Indications and Warning (I&W) of threatening activities
- Broad Area Search to locate the presence of target objects
- Focused Search to precisely locate, identify, and dynamically track individual targets
- Targeting of specific objects for defense or attack

Each of these functions must be performed for symbolic and cognitive objects, as well as for physical objects. The complementary roles and objectives for DIO and OIO (Table 2) require the fusion of data to detect and model targets in each domain and to model the relationships between domains. Data fusion at the symbolic level for example is applied to combine evidence from multiple network sources to detect and locate network intrusions for CND. Similarly, data fusion can support CNA by combining multiple sources to map networks and identify information targets for attack. At the cognitive level, data fusion provides the means to detect the presence of adversary denial and deception to protect own decision-makers' perceptions, while estimating the perceptions of an adversary decision–makers' perceptions in support of OIO deception and PsyOps.

Table 2 - The Functions Performed by Data Fusion in Information Operations

<table>
<tr><th colspan="2"></th><th>Defensive IO</th><th>Offensive IO</th></tr>
<tr><td colspan="2">The Role of IO …</td><td>Protect own information and information systems …</td><td>Attack adversary's information and information systems …</td></tr>
<tr><td colspan="2">… and the Objective</td><td>… to protect own decision-makers' perceptions</td><td>… to induce and coerce adversary decision-makers' perceptions</td></tr>
<tr><td rowspan="3">Functions in each Domain</td><td>Cognitive</td><td>• Detect denial and deception attacks on perception of own decision-makers using multiple sources to detect discrepancies, create deception hypotheses</td><td>• Detect, identify and target perceptions and mental states of adversary decision-makers using physical and symbolic evidence</td></tr>
<tr><td>Symbolic</td><td>• Detect, track and identify CNA intrusions from multiple network sources
• Track information object flows back to sources using multiple sources</td><td>• Search, detect, map, track and target adversary networks for CAN using multiple net sources
• Locate and target adversary information sources, sinks and stores</td></tr>
<tr><td>Physical</td><td>• Traditional detection and tracking of physical weapon platforms threatening own info systems</td><td>• Locate and target physical information systems and supporting resources (e.g. electrical power, communication, human administration personnel etc.)</td></tr>
</table>

While the data fusion functions and target modeling in these domains may be performed independently, as in the examples cited, we now consider how data fusion may be integrated across the three domains.

Three-Domain Data Fusion

Both DIO and OIO require integrated explanations of the objects of their operations, threats and targets, respectively. These explanations are provided by models – mathematical representations that estimate the existence (i.e. detection) and state (i.e. dynamic detection, or tracking, and identity) of the objects of operations. Two fundamental modeling alternatives may be considered:

- Integrated Causal Modeling- Models that depict events and their causal relationships across the domains can be constructed to relate observable events (physical, symbolic) to cognitive events, without modeling the states of each domain explicitly. Bayesian networks, for example, have been used to implement such models, representing the influence between events in the domains, without distinguishing the three domains or the states of objects in the domains.[18]
- Explicit Domain Models – This paper describes an explicit method of modeling each domain, and the interactions between domains using the JDL data fusion structure as the basis for the architecture. Distinct models of the objects, groups (of objects), and impacts in each of the three domains are maintained explicitly, to allow a complete accounting of all actors and influences.

The explicit model represents the states of objects in each domain, and their relationships. Observed phenomena are associated and combined (data fusion) to control the coupled models, even as radar detections are associated and combined to control a Kalman filter that estimates (models) the trajectory of an aircraft. Consider the simple example of a small military unit on patrol. Surveillance observations may report the time sequence of locations of the unit and the radio transmissions to base (physical and symbolic sources, respectively). These data may be able to model the trajectory of the patrol and their mission activities. From these models, we may be able to infer and then model the unit's (or unit leader's) emerging perception of the environment and perceived courses of action (decision alternatives) as the patrol unfolds. In this simple example, the unit leader's cognitive model is "driven" by the physical and symbolic models, which are in turn controlled by the surveillance sources.

The basic model framework required to describe the three domains must accept source data and maintain model that are integrated and consistent (Figure 3). The data fusion function accepts multiple sources in each domain and "drives" the model of the target. Physical sources of data at the physical level include direct physical observations by IMINT or SIGINT sensors, or by human observations. Symbolic sources include open data sources (OSINT, primarily electronic media), SIGINT and derived symbolic information (e.g. economic, inventory, demographic, and other abstract descriptions of the real world.) There exist numerous sources of cognitive data, used today: 1) behavioral observations are by psychologists to develop individual personality profiles, 2) focus groups, polls, surveys and other sampling methods are used by social scientists to profile the beliefs and mental states of populations, and 3) physical sensing of brain activity via Positron Emission Topography (PET), Magnetic Resonance Imaging (MRI), or Electroencephelogram (EEG) measurements are used for true remote sensing of cognitive activity in medical research applications. Only the first two are feasible sources of data for non-cooperative targeted individuals and populations – both are used today by politicians, intelligence analysts and IO practitioners.

The dynamic target model components at each level must allow interaction between models to assure a consistent explanation:

- A Priori Baseline - Models may establish baseline states for other domain models- initial conditions, a priori probabilities, etc. For example, the observed physical state of a military unit may establish the initial conditions for the state of the unit's technical sensor information (symbolic) and the unit's state of knowledge (cognitive).
- Cross-Inferencing - Each model may provide dynamic inputs to other layers to constrain, precondition or guide the other model layer. News reports (symbolic layer) may influence, and weather conditions (physical layer) may constrain the actions of a political party, for example. The inference paths proceed both upward and downward.
- Verification - Model states in one or two layers may be used to verify states in other domains. The estimated perception of a leader (cognitive domain) may be verified by comparing that perception with subsequent actions observed in the physical domain or statements made to the press (symbolic domain).

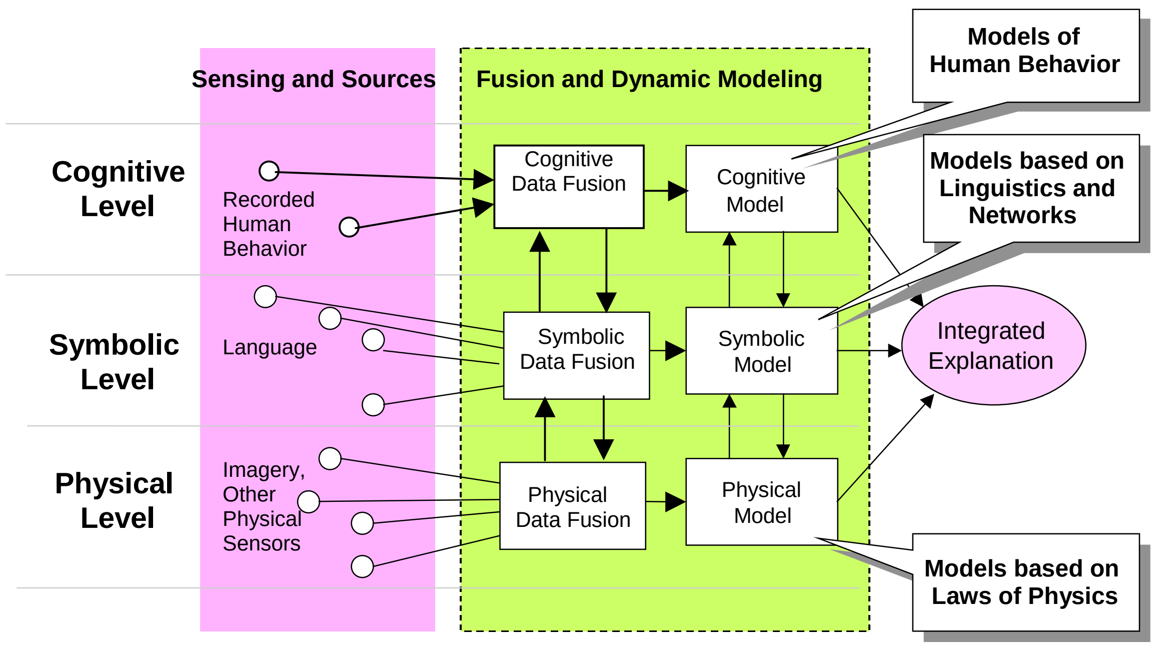


Figure 3- A Basic Three-Domain Data Fusion Architecture

Data Fusion Architecture for Three Domain Fusion

The basic structure for modeling target objects can be detailed (Figure 4) to illustrate the explicit data fusion (multiple source deduction) dynamic modeling approach at each of the three domains. The figure depicts a typical military battlefield surveillance application, with physical modeling of the terrain (in a Geographic Information System, GIS) and the military target objects, and symbolic modeling of military information flows ("conversations"). At the cognitive level, military commanders' beliefs and likely response plans are modeled. Both upward and downward inferencing (and validation) paths are required to maintain consistency across the domains. This basic structure (for individual target objects) is compatible with the U.S. DoD Joint Directors of Laboratories (JDL) data fusion model for level 1 object refinement [19].

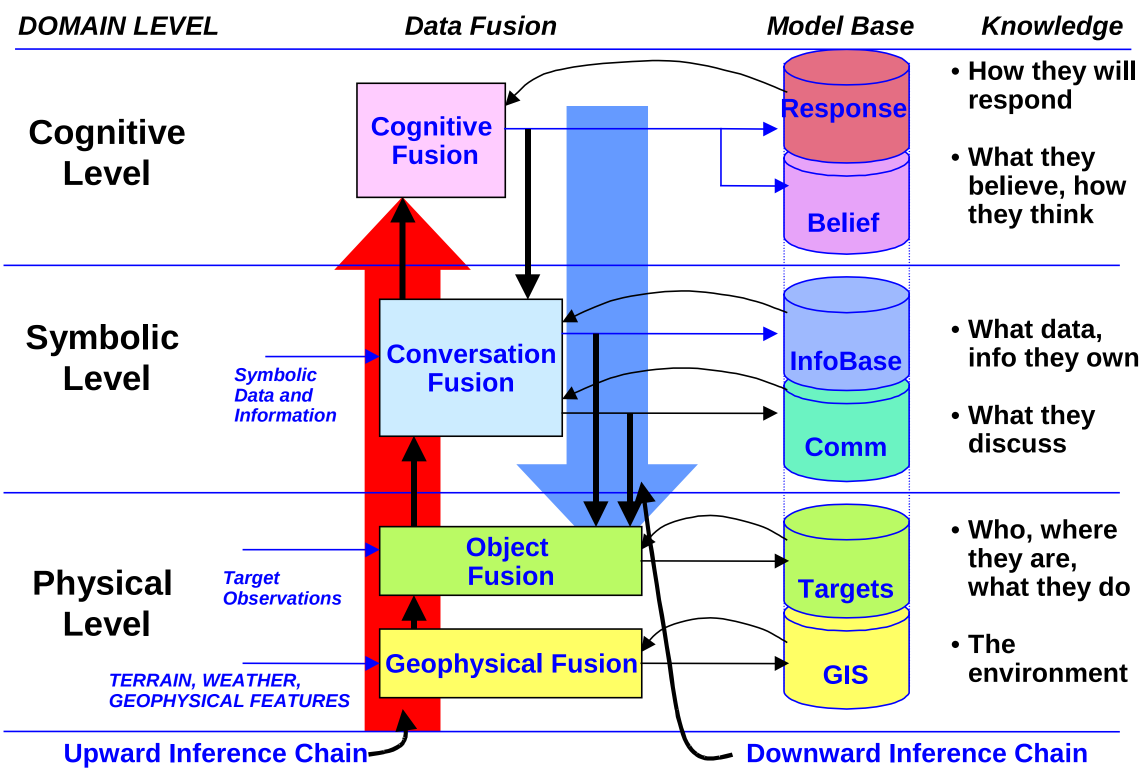


Figure 4- The Functional Components of a Three-Domain Architecture

This model can be extended to all three levels of the JDL model (Figure 5) to account for the modeling of the behaviors of individual objects, then groups of objects and their impacts on mission objectives. The architecture is organized by three levels of the JDL model: Level 1 combines data on individual target objects, Level 2 then aggregates the data target group (or situation) understanding, and Level 3 provides an understanding of impacts relative to the mission objectives of the observer.

The canonical architecture distinguishes:

- Fusion- The alignment, association and combination (fusion) processes at three JDL levels (L1 fusion of objects, L2 fusion of groups of objects, and L3 estimation of impacts). In this model the JDL process flows from detection of objects, to detection of groups and situations by relationships and behavior, to estimation of impacts by influences in context.

- Models - The dynamic models of reality being maintained at three JDL levels (M1 models of objects, M2 models of groups and M3 models of impacts, as illustrated in the figure as databases that maintain the current model states).

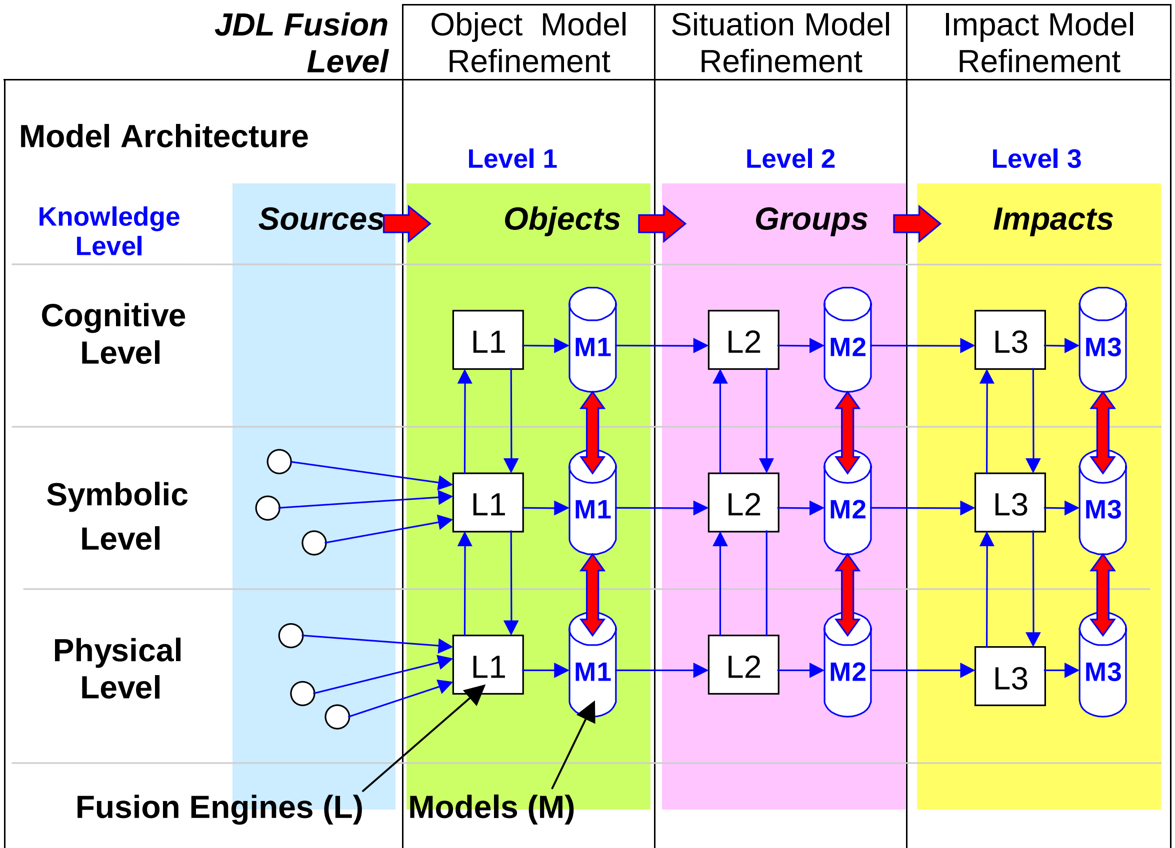
- Inference between Domains- The fusion over three domains of reality in which (at each JDL level) there exists upward (physical upward to symbolic then to cognitive) and downward (cognitive to physical) inference linkages. These linkages allow reconciliation, for example, between the observed physical state of a military force, the command information that that it is exchanging,, and the perception of it's situation (cognitive state) by military commanders.

Of course any practical implementation may not implement all of the models or fusion functions in the canonical architecture. In the battlefield example, many physical objects (e.g. tanks, trucks, tactical missiles, etc.) will be individually modeled and tracked at JDL level 1, but their cognitive counterparts (the individual humans operating them) will not be modeled at that level. The representative commander at the tactical unit level, may be modeled at JDL level 2, to estimate the mental state (with basic components of belief or perception, intentions, and desire-military mission objective) of the decision-maker.

The purpose of cognitive modeling in this architecture is to:

1) Provide an organized framework for understanding the potential mental states of the targeted adversary decision-maker(s),
2) Provide a structure for evaluating the influence of other domains on the decision-maker's perception, intentions and objectives, and,
3) Provide a means of visualizing and simulating the complex relationships between the many variables that influence human decision-makers.
4) Allow predictive analysis of the future mental states of the target (though there is no claim here to accurate prediction of human mental states, only feasible future mental states and state transitions and the ability to analyze future decision-making).

While human decision-making is complex, and may even exhibit irrational behavior, the model serves as a tool to aid the human analyst to explore causes and effects, alternative states and hypotheses. We do not suggest that such models will track mental states accurately as radar sensors track aircraft targets. We do submit that such models will enable IO analysts and operators to structure and better understand the more complex relationships between cognition and observations in the other two domains.



Modeled Military Objects (Targets)	**Cognitive Objects, Groups, Impacts**	Individual Decision-makers': • Perceptions • Mental states • Plans	Group (consensus situation): • Perceptions • Mental states • Plans	Predicted future cognitive states and decisions
	Symbolic Objects, Groups, Impacts	• Messages, • Information stored • Broadcasts • Data Collected	• Message traffic behavior, and networks • Message network	Predicted future information states (comm, processing behavior)
	Physical Objects, Groups, Impacts	Physical assets and actions • Facilities • Vehicles (air, land, sea) • People • Wpn Systems	Related sets (units) of physical assets: • Divisions • Brigades • Regiments • Garrisons	Predicted future physical states (unit behaviors)

Figure 5- The Three-Domain Architecture extended to model and explain objects, groups of objects and the impacts on each domain

The output of the three-domain model is a combined description of the states of cognitive, symbolic and physical objects, their states and the influences between them. The visualization of a representative military situation is illustrated in Figure 6.

The *physical view* includes the earth's surface, the location of natural and manmade features, military infrastructure, location of military units and operational activities. The emphasis of this view is the physical order of battle and physical constraints to movement and physical action. A GIS models the physical battlefield and provides for the integration of multiple layers of physical features in a single model. The GIS geolocates targets, land features, and situations in a common visual terrain reference.

The *symbolic view* describes the information flows, nodes and stores that are associated with the network structure of target C3I systems. The network description can be linked to the physical locations of the system components in the physical domain view. The Air Force is developing such symbolic level tools to model and visualize military communication and processing networks to visualization and simulation of network defense and attack effects.[20]

The *cognitive view*, depicts the cognitive states of the humans who perceive, reason and make judgements that influence the symbolic C3 I nets and the physical military orders of battle. This view visualizes the transition between mental states of military commanders, and the perceived decision trees for courses of action (COA's) that they may consider. The figure illustrates a visualization of the states (decision process) and COA's available to a commander at one node of a network (e.g. the unit commander of a missile battery within an integrated air defense network.) To create such a view, which is fully consistent with behaviors observed in the symbolic and physical domains, requires models of the cognitive processes of the targeted decision-makers.

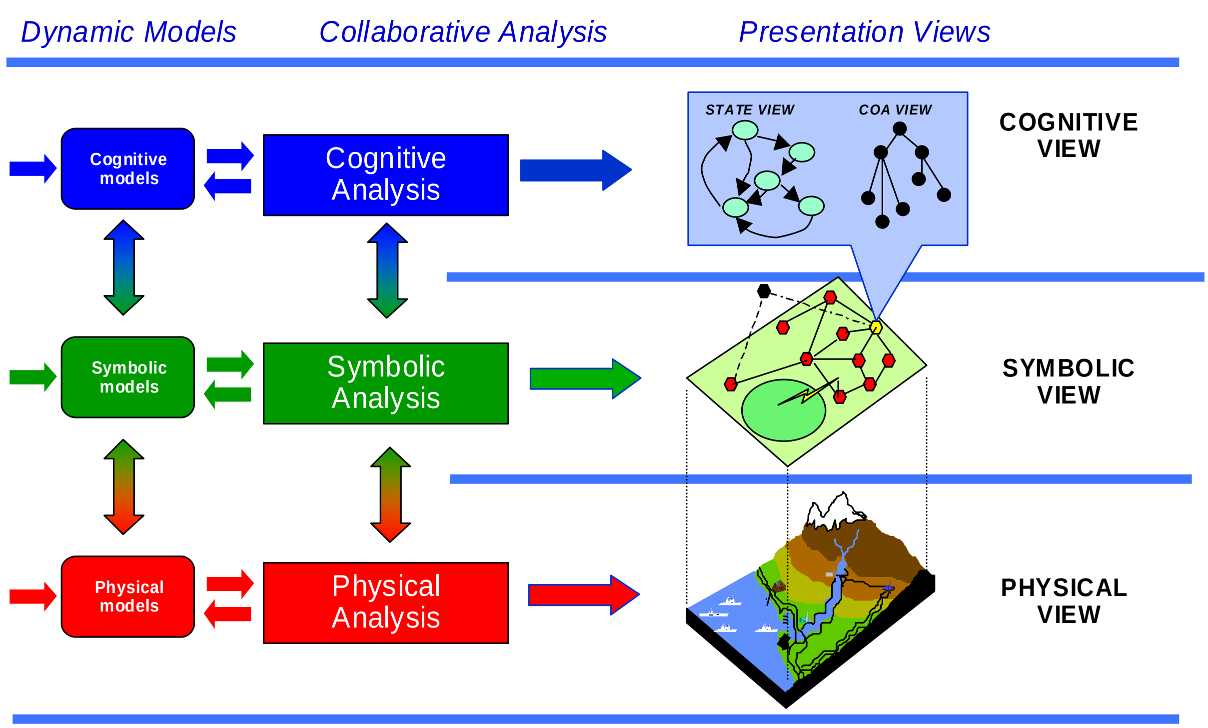


Figure 6 – Typical Presentation Views for a Three-Domain Military Model

Summary

Information Operations require the coordinated understanding of targets that exist in physical, symbolic information and human cognitive domains. Data fusion methods, developed over the past 20 years to model and explain physical targets, provide an excellent model for explicitly modeling real IO targets in the symbolic and cognitive realms that exist beyond the physical realm. Data fusion structures based on the JDL fusion model provide architecture to model and understand IO targets and threats within all three the domains of reality.

Endnotes

[1] IO definition from DoD Joint Publication JP1-02.

[2] Joint Vision 2020, US DoD Joint Chiefs of Staff J-5, 24 May 2000, page 28..

[3] Joint Vision 2010, US DoD Joint Chiefs of Staff, U.S. Government Printing Office, 1977.

[4] Waltz, Ed, "The Data Fusion Process: A Weapon and Target of Information Warfare" *Proc. of 10th National Symposium on Sensor and Data Fusion*, 14-17 April 1997.

[5] Waltz, Ed, "Information Operations: Creating New Frontiers for Data Fusion and Mining Technology " in *Proc. of 11th National Symposium on Sensor and Data Fusion*, May 1999.

[6] Waltz, Ed, "Information Operations: Integrating Offense, Defense and Dominance", in *Proc. of Protecting NATO Information Systems in the 21st Century*, NATO IST Panel Symposium, Washington DC, 25-27 October 1999.

[7] For a more thorough discussion of this concept, See: Waltz, Davenport, Johnson and Oxborrow, "The Critical Role of Cognitive Models in Next Generation Intelligence Architectures", in *Proc. of 8th Annual AIPA Symp*., Washington DC, 23-24 March 1998.

[8] The development of concepts of semiotics applied more generally to linguistics and human interpretation is attributed to Peirce's contemporary, Swiss linguist Ferdinand de Saussiere (1857-1913), and these works are applicable to the problems of perception management by the use of signs (symbolic objects) to influence thought (cognitive objects).

[9] Peirce, Charles Saunders, C.P. 1-480 - *The Logic of Mathematics*, 1896. In a manuscript a year later, Peirce further developed this triad, calling the cognitive object, the interpretant: "A sign, or representamen, is something which stands to somebody for something in some respect or capacity. It addresses somebody, that is, creates in the mind of that person an equivalent sign or perhaps a more developed sign. That sign which it creates I call the interpretant of the first sign." in C.P. 2-228 - *Division of Signs*, v. 1897.

[10] The term "target" is used throughout this paper to refer to the object of attention, not as a specific target of offensive attack (though this is one function of IO). The mind of an individual or a group is targeted as an object to be understood, modeled and explained by intelligence so actions can be taken. Actions to induce or coerce the mind of an individual or audience (group) also target the mind.

[11] Since Operation Allied Force, the U.S. DoD has considered refining the broad definition of IO to focus more narrowly on this cognitive aspect of IO, including perception management. See Verton, Dan, "DoD Redefining Information Operations", *Federal Computer Week*, 5-29-00.

[12] Quotation by Captain Sir Basil Liddell Hart in *Thoughts on War* (1944), cited in *Joint Doctrine for Information Operations*, Joint Pub 3-13, 9 October, 1998, page II-4.

[13] It should be noted that both domains could be considered to be "metaphysical", though classical philosophers would likely object. Both the cognitive domain, and the symbolic (entirely a product of human cognition, though represented in physical phenomena) are abstract in nature, transcend physical science and concern the mind.

[14] Liang, Qiao and Xiangsui, Wang, *Unrestricted Warfare*, (Bejing: PLA Literature and Arts Publishing House), February 1999, Preface.

[15] For basic view of escalation toward command and control warfare, See Waltz, Edward, *Information Warfare: Principles and Operations*, Artech House, 1998, page 28.

[16] Daniel, Donald C.F., Hayes, Bradd C., and Oudraat, Chantal de Jonge, *Coercive Inducement and the Containment of Crises*, (Washington DC: United States Institute of Peace Press), 1999.

[17] For descriptions of recent studies into the contrasting methods of inducement (confrontation) and shock and awe (violent cohercion), respectively, See: Howard, Nigel, *Confrontation Analysis: How to Win*

Operations Other than War, (Washington DC: CCRP), 1998, and Ullman, Harlan K. and Wade, James P., *Shock and Awe: Achieving Rapid Dominance*, (Washington DC: CCRP) 1996.

[18] Rose, Julie, A. and Smith, Wayne, L., " Influence Net Modeling with Causal Strengths: An Evolutionary Approach", in *Proc. Command and Control Research and Technology Symp.*, 1996.

[19] Steinberg, A., Bowman, C., and White, F., "Revisions to the JDL Data Fusion Model", Proc. of Joint NATO/IRIS Conf., Quebec City, Quebec, 19-23 October 1998.

[20] Daniel Verton, "Air Force to Build Info Ops System", Federal Computer Week, September 21, 1998, *http://athena.fcw.com/FCW/archive.nsf/Search+View/BE7747B0474C7CFC852566B1006D2AEB.*